

UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
YO998-529

Total Pages in this Submission

TO THE ASSISTANT COMMISSIONER FOR PATENTS

Box Patent Application
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

METHOD AND APPARATUS FOR SECURE AUTHORIZATION AND IDENTIFICATION USING BIOMETRICS WITHOUT PRIVACY INVASION

and invented by:

Timothy Joseph Chainer, Bruce P. Kitchens, Stephane Herman Maes, Marco Martens, Joseph Dela Rutledge, and Charles Philippe Tresser

If a **CONTINUATION APPLICATION**, check appropriate box and supply the requisite information:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: _____

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: _____

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: _____

Enclosed are:

Application Elements

1. ☐ Filing fee as calculated and transmitted as described below
2. ☒ Specification having 37 pages and including the following:
 - a. ☒ Descriptive Title of the Invention
 - b. ☐ Cross References to Related Applications (if applicable)
 - c. ☐ Statement Regarding Federally-sponsored Research/Development (if applicable)
 - d. ☐ Reference to Microfiche Appendix (if applicable)
 - e. ☒ Background of the Invention
 - f. ☒ Brief Summary of the Invention
 - g. ☒ Brief Description of the Drawings (if drawings filed)
 - h. ☒ Detailed Description
 - i. ☒ Claim(s) as Classified Below
 - j. ☒ Abstract of the Disclosure

JCS18 U.S. PTO
09/372170
08/11/99

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
YO998-529

Total Pages in this Submission

Application Elements (Continued)

3. ☒ Drawing(s) *(when necessary as prescribed by 35 USC 113)*
- a. ☐ Formal Number of Sheets _____
- b. ☒ Informal Number of Sheets 4 (Figs. 1-4)
4. ☒ Oath or Declaration
- a. ☐ Newly executed *(original or copy)* ☒ Unexecuted
- b. ☐ Copy from a prior application (37 CFR 1.63(d)) *(for continuation/divisional application only)*
- c. ☒ With Power of Attorney ☐ Without Power of Attorney
- d. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application,
see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference *(usable if Box 4b is checked)*
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ Computer Program in Microfiche *(Appendix)*
7. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all must be included)*
- a. ☐ Paper Copy
- b. ☐ Computer Readable Copy *(identical to computer copy)*
- c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

Accompanying Application Parts

8. ☐ Assignment Papers *(cover sheet & document(s))*
9. ☐ 37 CFR 3.73(B) Statement *(when there is an assignee)*
10. ☐ English Translation Document *(if applicable)*
11. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Acknowledgment postcard
14. ☐ Certificate of Mailing
- ☐ First Class ☐ Express Mail *(Specify Label No.):* _____

UTILITY PATENT APPLICATION TRANSMITTAL
(Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.
YO998-529

Total Pages in this Submission

Accompanying Application Parts (Continued)

15. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)

16. ☐ Additional Enclosures (please identify below):

Fee Calculation and Transmittal

CLAIMS AS FILED

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	48	- 20 =	28	x \$18.00	\$504.00
Indep. Claims	8	- 3 =	5	x \$78.00	\$390.00
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>					\$0.00
BASIC FEE					\$760.00
OTHER FEE (specify purpose)					\$0.00
TOTAL FILING FEE					\$1,654.00

- ☐ A check in the amount of _____ to cover the filing fee is enclosed.
- ☐ The Commissioner is hereby authorized to charge and credit Deposit Account No. _____ as described below. A duplicate copy of this sheet is enclosed.
- ☐ Charge the amount of _____ as filing fee.
 - ☐ Credit any overpayment.
 - ☐ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
 - ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).


Signature

Dated: August 11, 1999

Sean M. McGinn, Esq.
Registration No.: 34,386

CC:

Customer No.: 21254

MCGINN & GIBB, P.C.
A PROFESSIONAL LIMITED LIABILITY COMPANY
PATENTS, TRADEMARKS, COPYRIGHTS, AND INTELLECTUAL PROPERTY LAW
1701 CLARENDON BOULEVARD, SUITE 100
ARLINGTON, VIRGINIA 22209
TELEPHONE (703) 294-6699
FACSIMILE (703) 294-6696

**APPLICATION
FOR
UNITED STATES
LETTERS PATENT**

APPLICANTS: **Timothy Joseph Chainer, Bruce P.
Kitchens, Stephane Herman Maes, Marco
Martens, Joseph Dela Rutledge, and
Charles Philippe Tresser**

FOR: **METHOD AND APPARATUS FOR
SECURE AUTHORIZATION AND
IDENTIFICATION USING
BIOMETRICS WITHOUT PRIVACY
INVASION**

DOCKET NO.: **YO998-529**

METHOD AND APPARATUS FOR SECURE AUTHORIZATION AND IDENTIFICATION USING BIOMETRICS WITHOUT PRIVACY INVASION

BACKGROUND OF THE INVENTION

5

Field of the Invention

The present invention generally relates to a method and apparatus for authorization based on biometrics, and more particularly, to a method and apparatus for secure authorization using biometrics but without invasion of a subject's privacy. The invention is also equally applicable to other biometric functions such as identification.

10

Description of the Related Art

The need for personal recognition is a basic requirement of society which has existed for thousands of years. There are a number of activities in today's society which require identification including writing checks, making credit card purchases, authorizing a contract to purchase a home or car, obtaining pharmacological products, obtaining physical access to a building, submitting taxes, becoming married, etc.

15

Authentication techniques which an individual may use today can be divided generally into four major categories:

20

1) Something possessed - a physical object that a subject carries such as a key or a badge;

2) Something known - a password or personal identification number (PIN) or sequence which must be remembered, or answers to personal (or presumably familiar) questions or problems (e.g., birth date, mother's maiden name, etc.);

3) A physical characteristic - a fingerprint, hand geometry, retinal scan characteristics, dental records, facial characteristics, or voice features (vocal tract effect, pitch); and

4) Acquired characteristics - a manner of signing a document or of writing a text, accent, way of speaking (prosody, use of words etc.)

Some of the above methods require cooperation of the user (e.g., writing a text, answering a question, speaking, signing a document, undergoing a physical inspection such as for dental or retinal characteristics, etc.), while others can be more passively acquired. However, each method by itself has certain drawbacks.

For example, a key or badge is external to a person and can be lost, stolen or shared with other individuals, and therefore does not ensure that the person in possession of the key is the same person who is authorized to obtain access.

The use of passwords or PIN numbers has been accepted as one means

of personal identification. However, passwords must be remembered and can also be shared. Thus, security can be breached. Further, passwords preferably should be long for enhanced security protection. However, lengthy passwords are hard to remember. Moreover, the average number of passwords people have to remember is growing annually. This is problematic.

Examples of the proliferation of passwords include E-mail, Phone Mail, Bank ATM card, Credit Card PINs, Calling Card PINs, Internet Access Password, Stock Account Password, Bank account password, car alarm password, etc.; each is prevalent in society. As a result, account holders must physically record (e.g., write down) each of their passwords and PINs which is a clear threat to security.

Moreover, the use of a single password for several applications is often impossible as each application may assign a password or have different rules for the methods of selection and also the frequency with which passwords must be changed.

Further, in some cases, password protection has been compromised by thieves and others directly observing or filming passwords as they are being input (e.g., keyed in). These practices are used frequently to obtain calling card passwords, and may include use of false ATM machines, or phone line tapping.

A biometric print (i.e., stored in some database and used to perform biometric recognition) of a subject (e.g., person, animal, object, etc.) is based

on, in the case of a person, a unique physical characteristic such as a fingerprint, retinal pattern, DNA, hand geometry, dental characteristics, voice characteristics, and the like. It is unique (to a certain degree) and cannot be lost, stolen or shared with another person. Therefore, if used properly, it can
5 provide a higher level of security, or at least can be used as a basis for a mechanism for ensuring a higher level of security. Depending on the measured biometric, cooperation of the person may or may not be required.

However, acquiring biometrics of a subject typically requires the subject to perform an action. The advantage of this approach is that it only
10 works if the person chooses to cooperate.

Unfortunately, a major drawback of the use of biometrics is the loss of privacy that a person suffers when he/she provides a network or organization his/her biometric identity. Indeed, there have been many examples in society where personal information has been used by
15 organizations with dramatic negative impact on society. Therefore, in a democratic society, the need to provide a security for one's personal identity is and will continue to be important.

Furthermore, a common practice for many commercial corporations is to sell to other companies customer data including marketing surveys,
20 demographics, etc. As a result, many people are emphatic about not having their biometric characteristics known by such commercial companies nor any company (as any company can change policies or be purchased by another company with different moral and ethical standards).

Thus, prior to the invention, there has been no method or apparatus which can provide secure authorization using biometric information, while unobtrusively and non-invasively using biometric data in such a manner that the biometric data is not shared with another party (e.g., either a party requesting authorization or a third party).

SUMMARY OF THE INVENTION

In view of the foregoing and other problems of the conventional methods and systems, an object of the present invention is to provide a method and structure in which secure authorization is provided by using biometric information unobtrusively and non-invasively in such a way that there is minimal (or no) privacy invasion and such that the biometric data cannot be shared with a third party.

In a first aspect of the present invention, a method of authenticating a subject includes using one of a plurality of biometric measurements of a subject for authentication without the subject sharing their biometric data with another party (e.g., either the authorizing party such as the party requesting authentication or any other party).

In a second aspect of the present invention, a method of authenticating a characteristic of a subject includes using at least one of a plurality of authentication methods including personal information of the subject, a biometric of the subject, a password, and a secured card; and simultaneously

with the using of the at least one of the authenticating methods, the subject maintaining confidentiality of authentication material and withholding the material from any other party.

5 In a third aspect of the invention, a method for secure authentication of a subject includes selectively requesting any of passwords and knowledge-based information from the subject, and simultaneous with the selective request, interrogating a biometric of the subject, the biometric information being carried by the subject.

10 Thus, the present invention provides a system and method for using biometrics for verification without the invasion of privacy. The invention combines any of passwords, knowledge-based information and biometrics to provide secure and reliable authentication. Indeed, the invention, while using biometrics to generate a password, does so without an invasion of the subject's privacy.

15 Further, extremely reliable identification is provided by using the present invention. For example, a device could have several owners, producing a different password for each or the same one, depending on the application, provided that each owner's password is registered with the authorizing system and all biometric information is stored in the device, or
20 more generally accessible by the device. The local user's identity can be determined locally by having the user providing his/her user ID or by biometric identification of the user among the enrolled authorized users. The identification stage can be implemented by producing, for example, a set of N

best matches for N subsets. The index formed by concatenation of the N indices can uniquely identify the user. This enables not only authentication, but also prior identification of the user without transmission of the biometrics.

5

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other purposes, aspects and advantages will be better understood from the following detailed description of a preferred embodiment of the invention with reference to the drawings, in which:

10

Figure 1 displays the overall structure of a device 100 according to the present invention;

Figure 2 is a flowchart illustrating how a device 100 according to the present invention is initialized and how a subject's biometrics are stored in a memory incorporated in the device 100 according to the present invention;

15

Figure 3 illustrates a flowchart of the inventive method 300 of authentication; and

Figure 4 is a block diagram of the inventive device 100 showing how authentication is performed according to the preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS OF THE INVENTION

Turning now to the drawings and more specifically to Figures 1-4,
embodiments of the present invention will be described below. It is noted
5 that, for consistency and ease of understanding, the same reference numerals
are used to designate like elements throughout the drawings.

First, it is noted that the present invention, in the preferred
embodiments, will use some standard methods from modern cryptography. A
description of the specific cryptographic techniques used in this disclosure
10 (SK/PK pairs and hash functions) can be found in "Handbook of Applied
Cryptography", by Alfred J. Menezes, Paul C. van Oorschot and Scott A.
Vanstone, CRC Press, 1997.

It is noted that, e.g., by using some zero-knowledge protocol, a Smart
card can be authenticated but cannot be duplicated, and the authentication
15 may have no access to some of the information stored in the Smart card, while
this information can be used during the usage of the Smart card, to generate
other information. This property is what the present inventors consider to be
the characterization of a smart card, for purposes of the present application.
Accordingly, in the present disclosure, any electronic component with these
20 properties and with some memory and/or some processing capabilities, will
be called "a smart component" or "a Smart card", even if it does not actually

take any form resembling a “card”. A general reference to Smart card technology and applications can be found in “Smart Cards: A Guide to Building And Managing Smart Card Applications” by Henry Dreifus and J. Thomas Monk, John Wiley & Sons, 1998.

5 Additionally, it may be described below that a card or some other device is *uniquely recognized by some external reader*. For such an operation, a variety of methods allowing such unique recognition are well known to people ordinarily skilled in the art of security protection, using either pure cryptography, tagging methods, or a combination thereof.

10 With reference now to Figure 1, a device 100 is shown according to the present invention. It is noted that the device 100 optionally may be a portable unit or a non-portable unit depending upon the designer’s constraints and requirements. Further, the device 100 may take the form of a Smart card, a personal area network (PAN) tool, an apparatus, such as a
15 computer or a terminal, linked (e.g., either by wire or wireless communication) to a network.

 According to the invention, the device 100 includes at least one sensor 110, and more preferably a plurality of sensors 110, each of which is sensitive to some form of biometrics (or a plurality thereof for multiple
20 function sensors).

 The device 100 further includes at least one processor 120 for analyzing biometric data so as to encode and authenticate them, building an encoded password out of biometric data, and generating further

authentication.

For example, the sensor 110 can capture finger print(s) data in the form of the minutia coordinates, say each coordinate being defined with four digits. In 120, these numbers are then concatenated to form a master number N, and a secure hash function, another form of encryption, can then be used to produce the encoded password of the device itself in case enhanced security is desired. 120 also executes other typical tasks depending on the application.

For instance, “further authentication” of the device (e.g., card etc.) itself can be a second secret password attached to the device and “some other typical task” may include computing a password depending on the date and time and on the first and/or the second above mentioned secret passwords.

Additionally, device 100 includes at least one memory (or a general data storage device) 130, and a power source 140 and/or contact allowing use of an external power source (e.g., household AC circuit, DC power source, etc.).

Further included is a contact and/or a contact-less external control apparatus interface 150 (communication unit), allowing the device to communicate with an external control apparatus. The external control apparatus may be linked to a world wide network such as the World-Wide-Web or Internet, or to a local area network (LAN) through a reader 152. The reader 152 may be connected to an authentication server 154, as shown in Figure 1.

For enhanced security, a non-duplicable authenticating tag 160 may be provided.

Depending on the application, one or several biometrics may be selectively employed. More particularly, for data such as fingerprints, in some cases vital signs would also be registered to assure that the authentication being performed is of a live human being. Such registration would not be as important in the case of signature strokes.

Additionally, for increased security and reliability, a plurality of biometrics might be used if the biometric is likely to be affected by external circumstances (e.g., the voice being affected by a cold, the strokes of a signature/writing sample being changed after a wrist injury, etc.).

Each of the chosen biometrics will be initialized as follows.

Figure 2 shows a flowchart of a method 200 for initializing the biometrics to be used. In step 201, at a first use of the device 100, the biometric is detected by an appropriate sensor 110 (one of the sensors at 110 in Figure 1), the data from the sensor are digitized, and, optionally, encrypted in the processing unit 120.

In step 202, the digital message so composed is stored in a data storage unit 130, corresponding to the appropriate one of sensors 110 (i.e., different sensors correspond to different addresses of data storage or different data storages).

After completion of this storage, in step 203, the stored data are protected so that attempting to reinitialize the process would invalidate the

device. For example, the data could be protected by storing the data together with a secretly encrypted form of it. The authentication process will use the corresponding publicly known key. Another possibility is that the data could be written in a one-time write operation.

5 Thereafter, the device (card) is initialized. As shown in steps 204-210, there are two possible modes of initializing a device (e.g., a “Smart Card” or more generally a “Smart Device”, etc.).

 In a first mode (e.g., see steps 205-207), the owner opens an account “in person”, perhaps by making an initial deposit, or by identifying
10 him(her)self by some other means (e.g., a single-use PIN), as shown in step 205. A card (or more generally a device) is issued, and the owner uses it to produce a password depending on his (her) biometric, in step 206. The password is stored in the authenticating system, in step 207. Then, this is the password for that account, to be accepted thenceforth.

15 This system does not require any (but is compatible with) storage of biometric data in the device (card).

 In a second mode (as in steps 208-210), the card (or more generally a device) is provided (e.g., by some secure means) to the owner with a password already installed which is known to the authenticating system (step
20 208). The owner initializes the card as described above, storing biometric data (step 209) by which, at each use, the card recognizes its owner and produces its pre-authorized password. Similarly, the card can protect the biometric data on the card (step 210) by destroying or nullifying the card if it is reinitialized.

However, the second mode has several drawbacks. For example, if the card is intercepted enroute to the proper owner, then it can be used freely by the interceptor. Secondly, once initialized, it contains the biometric data, though probably in encrypted form.

5 The first drawback can be an advantage from a privacy and convenience perspective. That is, the owner need not be otherwise identified to the authorizing system. The possession of the uninitialized card is sufficient.

10 With both the first and second modes for initialization, the actual generation of the password can be more involved, to avoid in particular counterfeiting on the basis of eavesdropping to get the password being transmitted.

15 For example, public key encryption can be used to generate an actual password on the basis of a “base” password (e.g., protected by the Smart card architecture for instance) and the present time. As public encryption is used, the eavesdropper cannot get back to the base password, while the addressee of the computed password, who is the generator of that public key encryption scheme, possesses that private part and can access the base password. The computed password cannot be reused as time changes.

20 To avoid even the improbable (because difficult) case of instant reuse, a transaction number can also be incorporated with the time and the base password to generate the transmitted password.

When the user receives the device 100, he (she) will perform a remote

authentication with an authentication server 154 (shown in Figure 1), to unlock the device (or to receive an authorization number that will unlock the device). Such concepts are described in the above-described U.S. Patent Application No. 08/873,079, filed on June 11, 1997, having IBM Docket No.

5 Y0997-136, entitled "PORTABLE ACOUSTIC INTERFACE FOR REMOTE ACCESS TO AUTOMATIC SPEECH/SPEAKER RECOGNITION SERVER", and in U.S. Patent Application No. 08/008,122, filed on January 16, 1998, having IBM Docket No. Y0997-258, entitled "A PORTABLE INFORMATION AND TRANSACTION PROCESSING
10 SYSTEM AND METHOD UTILIZING AUTHORIZATION AND DIGITAL CERTIFICATE SECURITY", each incorporated herein by reference.

Referring to Figures 3 and 4, a method 300 and a system 400, respectively for performing the authentication procedure are shown and described hereinbelow. Such a method could be performed for one or more
15 sorts (types) of biometric data that is being used in the transaction. For example, first fingerprints could be analyzed, then the method could be performed for voice, etc. The conjunction of such readings of different biometrics can also be used to ensure that the person is alive. It is noted that several sensors may be used which must work simultaneously, such as
20 fingerprint and heart beat sensors.

In Figure 3, in step 301, a sensor 110 (e.g., one of those at 110 in Figure 1) captures the corresponding biometric and transmits it to a processing unit 120 (e.g., one of those at 120 in Figure 1) which treats it in

the same way as the processing unit at the time of initialization. The processor 120 stores the biometric in a register (or memory) for later comparison with what is stored in the data storing unit.

Then, in step 302, the ensuing digital stream is compared with what is stored in a data storing unit 130 (e.g., one of those at 130 in Figure 1).

In step 303, if the processing unit 120 decides there is no match, then in step 304 no authentication occurs and the process ends. Alternatively, instead of ending the process, the process could continue to step 305 and the user could be prompted to use an alternate biometric when desirable by the application and loop to step 301.

If there is a match in step 303, then in step 306 the processing unit 120 commands another processing unit 120 (e.g., one of the processors 120 in Figure 1; alternatively the same processor 120 which received the biometric data) to encode the stored biometric data to compose a password. It is noted that, since it is the stored data which is used each time, the password is the same at each usage. The same would be true for biometric data which can be read in an exactly reproducible manner.

Then, in step 307, this password is passed/transmitted to the communication unit 150 (e.g., one of the external control apparatus interface(s) 150 in Figure 1). Optionally, in step 308, the public key encryption scheme to generate a transmitted password on the basis of a base password, as described above, can be used here.

Alternatively, in step 308, to complete the authentication in cases

when more security is needed, the device itself can be identified. This prevents a problem such as a “false ATM”, where the authentication message is captured and then reused without using the original device. This can be performed using zero knowledge protocol (e.g., see Cryptography: Theory and Practice, Douglas R. Stinson) or some other form of cryptography-based authentication, such as a coding algorithm which depends on the device and cannot be read from the device, or using some form of physical irreproducible authentication 160, as disclosed, for example, in U.S. Patent No. 5,581,257 to Greene et al., incorporated herein by reference, in which radio frequency (RF) automatic identification systems have been proposed as a general purpose authentication system.

Such a system offers high security, and has been proposed for the protection of identification documents, credit cards, and money. The essence of this system is the existence of processes which generate one of a kind, non-duplicable, samples of some materials, so that the samples can be identified by some reading mechanisms. From this point of view, the use of inhomogeneous media in U.S. Patent No. 5,790,025, incorporated herein by reference, is another instance of the same concept.

An important aspect of the invention is that biometric data verification is done by whoever needs to use an authentication. Then, this biometrics verification activates a password-controlled authentication mechanism which does not transfer enough information for the biometrics to be revealed. The entire system optionally can be carried, together with the recognition

mechanism, on a tool that belongs to the person who wishes to use such a biometrics-based identification mechanism. (Of course, as mentioned above, the system could be non-portable and need not be carried by the user.)

For instance, in one preferred embodiment, a compact device (about
5 the size of a credit card in the case of a Personal Area Network (PAN) tool as described in U.S. Patent No. 5,790,827, incorporated herein by reference, or a Smart card), is provided which is able to read a specified biometric (e.g., fingerprints, voice, DNA-information, signature, etc. or a combination thereof), and produce the password needed, preferably using some encryption
10 and/or secure hashing.

Preferably, this device is owned by the person to be authorized to do some task. The procedure of authorization will be implemented, for example, as described below.

First, at the moment of authorization the person puts the device (or
15 inserts it partially, or slides it through a reader, or presents it to a reader for remote reading) into the machine which prompts for a password for some authorization to be given. The device will read the biometrics (or some number of them) using some sensor (or a plurality of them) included in the device and compute the password.

20 Then the device will let the password be read by the authorizing machine (e.g., in a contact or contact-free manner).

The method described above implies usage of a hashing/mapping method which is stable with respect to the variations of the biometrics

extracted at recognition. One possible way to achieve some stability includes mapping regions of the biometric-print space, to key/password generating rules. These rules can also be simultaneously be modified by PIN, password or answers to personal questions. That is, the result of the biometric measurement can be mapped to a password or a key. Unfortunately, biometric prints may be noisy and unstable. Thus, the invention desires to define a set of regions stable enough so that mapping can be built between these regions and the resulting password.

Alternatively, the stability is achieved by storing on the device the biometric-prints of the user (e.g., or each of a plurality of users if the device has multiple users). Different conventional hardware and software security solutions can be used to protect access to the stored template. Smartcard architectures are good examples on how to achieve such secure storage.

It is also possible to encrypt the biometric-print using the user's biometric and personal knowledge (which can also be done in conjunction with the use of Smart card technology). This approach is described in U.S. Patent Application No. 09/240,214, filed on January 29, 1999, having IBM Docket No. YO0998-334 and entitled "BIOMETRIC AUTHENTICATION SYSTEM WITH ENCRYPTED MODELS", incorporated herein by reference.

Of course, the storage of a local biometric-print forbids remote authentications of the user. This is especially acute for telephone-based voice authentication. That is, the service provider would still need to store locally the users' voice print.

As a first solution to the above problem, an acoustic coupler could be used as described in U.S. Patent Application No. 08/873,079, filed on June 11, 1997, having IBM Docket No. Y0997-136 and entitled "PORTABLE ACOUSTIC INTERFACE FOR REMOTE ACCESS TO AUTOMATIC SPEECH/SPEAKER RECOGNITION SERVER", incorporated herein by reference. However, the verification would be performed locally as disclosed in the present invention, and only a binary password or logon-procedures would be transmitted, instead of the acoustic features for a networked verification.

Another solution is proposed using compressed biometrics in U.S. Patent Application No. 08/126,894, filed on July 31, 1998, having IBM Docket No. Y0997-252, entitled "SYSTEM AND METHODS FOR COMPRESSING BIOMETRIC MODELS", incorporated herein by reference. Instead of storing the biometric (encrypted or not, locally or on the network), a user's biometric-print is measured by ranking biometric prints of N subsets of M biometrics. The index of the top ranking speaker for each of the N subsets can be used as elements of the key generation or password generation procedure. Order of the bit contributions, indexes of the speakers in each subset, amount and composition of the subsets are all elements which can be uniquely associated to a service provider and can even be determined individually user by user or on the basis of other external information like password or personal information.

For further protection of privacy, the device can also compute a new

password, by some function whose inverse is not effectively computable, out of key generation described above.

For enhanced security, the device also may carry a unique non-duplicable authentication mechanism, which may be constructed so as to be completely independent of the biometric. The password (or a plurality thereof) may for instance be an encrypted version of the biometric. Again, what is most important for the sake of privacy protection is that the authorizing machine will not have any access to the biometric itself.

The device cannot be used by anyone other than the owner, since the password is not stored in the device, at least not in an accessible way as described below, and the device will produce the correct password only when it can read the biometrics from the owner.

However, a device could have several owners, producing a different password for each or the same one, depending on the application, provided that each owner's password is registered with the authorizing system and all biometric information is stored in the device, or more generally accessible by the device. The local user's identity can be determined locally by having the user provide his/her user ID or by biometric identification of the user among the enrolled authorized users.

The identification stage can be implemented as described in the above-mentioned U.S. Patent Application No. 08/126,894, incorporated herein by reference. It produces a set of N best matches for the N subsets. The index formed by concatenation of the N indices can uniquely identify the

user. This enables not only authentication, but also prior identification of the user without transmission of the biometrics.

Further, a smart card, PAN tool, etc. containing a reader for fingerprints could be usable together with vital signs readers.

5 Additionally, a smart card, PAN tool, etc. could be connected to a pen for recording the strokes of the signature of the person as he/she signs their name and could be used with signature verification. To verify a signature, a data input pen as described in U.S. Patent No. 4,513,437 to Chainer et.al., incorporated herein by reference, could be used which contains two
10 accelerometers which measure the acceleration along two perpendicular axes of the pen body and a derivative of force sensor which measures the rate of change of force of the pen to the paper.

 The signals are sampled while signing, and can be input to the smart card for comparison with an encrypted reference of the person's signature
15 dynamics. Storing encrypted biometric information on smart cards is described by Abraham et. al., IBM Systems Journal Vol. 30, No. 2, 1991. The data input pen produces signals while signing on any surface. Therefore, only a cable or radio frequency (RF)-type connection with the card would be necessary.

20 Alternatively, the device (e.g., smart card, etc.) could contain an x - y grid, and the signature dynamics would be recorded on a grid-crossing surface which provides x , y and time location of the pen tip to provide dynamic signature data to the card.

Such devices could be used for instance to gain access to machines such as ATM-machines, but neither the ATM-machine nor the bank will know the fingerprint.

Another example of use of this invention is a biometric-based single sign-on system. Indeed, once a password generation mechanism is designed which allows the use of robust hash/mapping of the test biometric-print, hash/mapping of a securely stored local biometric-print or hash/mapping of a compressed biometric-print as described in the above-mentioned U.S. Patent Application No. 08/126,894, incorporated herein by reference, all the ingredients are present to provide a biometric single sign-on service. For a given user, a Java®, HTTPD and Windows® password request can be identified automatically, or if needed, hand-tagged by the user. Requests from unknown providers induce the generation of a new password along with its appropriate biometric-print-to-password map.

The map is encrypted and stored locally along with a user/logon-ID and the identification of the logon page or other signature of the authentication request from the service in question. The user always has the option to over write the logon-ID and password to suit his preferences or the requirements of the service provider. The correction is also stored as additional mapping. Upon receiving a request, the system checks if the requestor is already assigned a password.

If a password already has been assigned, the system automatically and transparently logs the user-in, possibly after asking confirmation from the

user, otherwise, it generates a new password as described before.

With a conventional single sign-on solution adding biometrics to the authentication procedure, the single sign-on manager can be run locally on the user's work station, instead of being distributed. Should distribution be
5 needed, the private biometric approach can be used to maintain privacy.

Further, with the approach of the present invention, knowledge-based information and passwords can be treated like biometric-prints. In degenerate cases, the system might use only one of these security mechanisms.

In the case of multiple sign-on for instance, the sensor will not
10 necessarily be included in the device, or an alternate sensor will be used which communicates with the device so that the device can be kept in a pocket.

For example, if a user works with a computer which serves as a terminal for many applications, the user can use a PAN tool and have some
15 biometric data read each time a new application needs authentication, for example by simply using a sensor attached to the terminal. The reading is transmitted to the PAN tool where the verification is made and the appropriate password(s) is (or are) generated.

As still another use, the device can generate audible signals which can
20 be transmitted over telephone lines to allow the user to identify himself/herself on the telephone without giving out his/her biometric data (e.g., the telephone used can be such that it distorts such identifying personal characteristics, but still allows the recognition of the signal generated by the

device). This is an extension of the above-mentioned U.S. Patent Application No. 08/873,079.

Along with the above, the present invention may be utilized in combination with a method to perform text-independent speaker recognition, as described in U.S. Patent Application No. 07/788,471, filed on January 28, 1997, and having IBM Docket No. Y0996-188, entitled “TEXT-INDEPENDENT SPEAKER RECOGNITION FOR TRANSPARENT COMMAND AND CONTROL AMBIGUITY RESOLUTION AND CONTINUOUS ACCESS CONTROL”, a method to add knowledge-based information, as described in U.S. Patent Application No. 08/871,784, filed on June 11, 1997 and having IBM Docket No. Y0997-138, entitled “APPARATUS AND METHODS FOR SPEAKER VERIFICATION/IDENTIFICATION/CLASSIFICATION EMPLOYING NON-ACOUSTIC AND/OR ACOUSTIC MODELS AND DATABASES”, and a random question based access control system, as described in U.S. Patent No. 5,774,525, entitled “METHOD AND APPARATUS UTILIZING DYNAMIC QUESTIONING TO PROVIDE SECURE ACCESS CONTROL”, all incorporated herein by reference.

Thus, with the invention, a subject can be authenticated/identified and yet the subject’s privacy remains intact. That is, a device, which may or may not be portable depending on its configuration, can authenticate a subject by asking the subject a question, measuring a biometric, etc., to produce a password, and subsequently the password is provided to an entity requiring

the authentication/identification.

While the invention has been described in terms of several preferred embodiments, those skilled in the art will recognize that the invention can be practiced with modification within the spirit and scope of the appended claims.

For example, in the invention, questions may be asked to the user (subject) for the local authentication. The answer may be based on the history of the previous authentication. Thus, it may be useful to store locally (e.g., at the subject's side) information about the last (previous) authentication. Further, it may be desirable to periodically update the biometric print to prevent an "aging" effect.

For example, the invention can be applied to a steering wheel to develop a "Smart steering wheel". In such a case, the user would grip the steering wheel, and the user's fingerprints would be read. If the fingerprints match an identification profile of the user, then the car is rendered operable (e.g., started, etc.).

The inventive concept could also be applied to firearms. For example, a "Smart pistol" could be implemented in which the user would grip the pistol grip, and the user's fingerprints would be read. If the fingerprints match an identification profile of the user, then the pistol would be rendered operable.

CLAIMS

What is claimed is:

- 1 1. A method of authenticating a subject, comprising:
 - 2 using one or a plurality of biometric measurements for authentication
 - 3 without any sharing of the subject's biometric data.
- 1 2. The method according to claim 1, further comprising:
 - 2 storing said biometric data in an individual unit, said individual unit
 - 3 belonging to said subject.
- 1 3. The method according to claim 2, wherein said individual unit is portable
 - 2 for being carried by said subject.
- 1 4. The method according to claim 2, wherein said individual unit is non-
 - 2 portable.
- 1 5. The method according to claim 2, wherein said individual unit comprises
 - 2 one of a smart card, a personal area network (PAN) tool, and an apparatus
 - 3 linked to a network.
- 1 6. The method according to claim 1, further comprising:

2 after said authentication, selectively obtaining access to any of a
3 location, a service, and an option in a service by said subject.

1 7. The method according to claim 1, further comprising:
2 generating at least one of a password and another authentication
3 procedure based on biometric authentication locally under the subject's
4 control.

1 8. The method according to claim 7, further comprising:
2 securely storing the biometric on an apparatus carried by said subject.

1 9. The method according to claim 1, further comprising:
2 generating at least one of a password and another authentication
3 procedure based on at least one biometric feature extracted locally under the
4 subject's control.

1 10. The method according to claim 9, wherein said generating is performed
2 without storing the subject's biometric feature.

1 11. The method according to claim 9, further comprising:
2 deriving said at least one of the password and the another
3 authentication procedure from the biometric extracted locally when
4 authentication is required.

1 12. The method according to claim 7, further comprising:
2 deriving said at least one of the password and the another
3 authentication procedure from compressed biometrics extracted locally under
4 the subject's control or from a network, when authentication is required.

1 13. The method according to claim 7, further comprising:
2 managing multiple passwords and authentication procedures, by at
3 least one of:
4 monitoring an authentication request;
5 identifying a requestor;
6 generating at least one of a new password and an
7 authentication procedure for a new requester;
8 storing the authentication procedure generation method and
9 the identity of the requestor in a secure manner; and
10 authenticating the user for known requesters using the stored
11 procedure and the result of the local authentication procedure.

1 14. A method of authenticating a characteristic of a subject, without
2 compromising privacy of the subject, comprising:
3 using at least one of a plurality of authentication methods including
4 personal information of the subject, a biometric of the subject, a password, a
5 personal identification number (PIN) and a secured component; and

6 simultaneously with said using, said subject maintaining
7 confidentiality of authentication information and withholding said
8 authentication information from the other party.

1 15. The method according to claim 14, further comprising:
2 generating at least one of a password and another authentication
3 procedure based on authentication locally under the subject's control.

1 16. The method according to claim 15, further comprising:
2 securely storing authentication information on an apparatus locally
3 under the subject's control.

1 17. The method according to claim 15, further comprising:
2 deriving said at least one of the password and the another
3 authentication procedure from the local authentication when authentication is
4 required.

1 18. The method according to claim 16, further comprising:
2 securely storing the authentication information on the apparatus using
3 at least one of a knowledge-based information, a possession-based
4 information, a password-based information, and a biometric-based
5 information.

1 19. The method according to claim 14, further comprising:
2 selectively completing the authentication with a remote service using
3 a communication port and protocol.

1 20. A method for secure authentication of a subject, comprising:
2 selectively requesting any of a password and a knowledge-based
3 information from said subject; and
4 simultaneously with said selectively requesting, interrogating
5 biometric information of the subject, said biometric information being carried
6 by said subject.

1 21. The method according to claim 20, further comprising:
2 using said biometric information to generate said password.

1 22. The method according to claim 20, further comprising:
2 performing biometric data verification by a device associated with
3 said subject,
4 wherein said biometric data verification activates a password-
5 controlled authentication mechanism which transfers information, but which
6 withholds sufficient information so that the biometric is not revealed, to a
7 party requiring authentication.

1 23. The method according to claim 21, wherein obtaining said password is

2 performed by using at least one of an encryption and secure hashing.

1 24. The method according to claim 20, wherein a device is carried by the
2 subject to be authorized to perform a task,
3 wherein at a moment of authorization, said device is presented to a
4 reader of an authorizing machine of an entity seeking authentication, which
5 prompts said device for a password for authorization to be given, and
6 wherein said device reads a biometric of said subject using a sensor
7 included in the device and computes the password.

1 25. The method according to claim 24, wherein said device allows the
2 password to be read by the authorizing machine.

1 26. The method according to claim 25, wherein said password is read in a
2 contacting manner.

1 27. The method according to claim 25, wherein said password is read in a
2 contact-free manner.

1 28. The method according to claim 24, further comprising:
2 using one of a hashing and a mapping technique, which is stable with
3 respect to variations of the biometric extracted, said using including mapping
4 regions of a biometric-print space, to the password having been computed.

1 29. The method according to claim 28, wherein said using includes:
2 measuring a biometric-print of the subject by ranking biometric prints
3 of N subsets of M biometrics,
4 wherein an index of a top ranking of each of the N subsets is used in
5 computing the password.

1 30. The method according to claim 24, further comprising:
2 storing on the device information regarding a previous authentication
3 including a biometric-print of the subject.

1 31. The method according to claim 20, further comprising:
2 encrypting a biometric-print using the subject's biometric and
3 personal knowledge onto a device carried by said subject.

1 32. The method according to claim 20, further comprising:
2 providing a unique non-duplicable authentication mechanism on a
3 device associated with said subject, said authentication mechanism being
4 constructed so as to be completely independent of the biometric,
5 wherein said authentication mechanism is prevented from accessing
6 the biometric itself.

1 33. The method according to claim 32, wherein said device associated with

2 said subject produces a correct password only when the device reads a
3 biometric from the subject.

1 34. The method according to claim 20, wherein biometric information for a
2 plurality of subjects is stored in a device associated with the subject.

1 35. An apparatus for secure authentication, without compromising privacy of
2 a subject, comprising:

3 a reader, associated with the subject, for reading a specified biometric
4 of said subject; and

5 a password generator for producing a password needed based on said
6 biometric.

1 36. The apparatus according to claim 35, wherein said password generator
2 includes an encryption device using at least one of encryption and secure
3 hashing.

1 37. An apparatus for secure authentication, comprising:

2 means, associated with a subject, for reading a specified biometric of
3 said subject; and

4 means for producing a password needed based on said biometric,
5 without providing access to said biometric by anyone other than said subject.

1 38. The apparatus according to claim 37, wherein said means for producing
2 said password includes an encryption device using at least one of encryption
3 and secure hashing.

1 39. A method of identifying a subject, comprising:
2 using one or a plurality of biometric measurements for identification
3 without any sharing of the subject's biometric data.

1 40. The method of claim 39, wherein a subject's identity is determined
2 locally, under the subject's control, by having the subject provide at least one
3 of a user ID and by biometric identification of the subject among enrolled
4 authorized subjects, and
5 wherein said identification produces a set of N best matches for N
6 subsets, and an index formed by concatenation of the N indices uniquely
7 identifies the subject.

1 41. A method for identification of a subject, comprising:
2 selectively requesting any of a password and a knowledge-based
3 information from said subject; and
4 simultaneously with said selectively requesting, interrogating
5 biometric information of the subject, said biometric information being carried
6 by said subject.

1 42. The method of claim 41, wherein a subject's identity is determined
2 locally, under the subject's control, by having the subject provide at least one
3 of a user ID and by biometric identification of the subject among enrolled
4 authorized subjects, and
5 wherein said identification produces a set of N best matches for N
6 subsets, and an index formed by concatenation of the N indices uniquely
7 identifies the subject.

1 43. An apparatus for identification of a subject, comprising:
2 a reader, associated with the subject, for reading a specified biometric
3 of said subject; and
4 a password generator for producing a password needed based on said
5 biometric.

1 44. The apparatus according to claim 43, further comprising:
2 means for storing data of said biometric in an individual unit, said
3 individual unit belonging to said subject.

1 45. The apparatus according to claim 44, wherein said individual unit is
2 portable for being carried by said subject.

1 46. The apparatus according to claim 44, wherein said individual unit is non-
2 portable.

- 1 47. The apparatus according to claim 44, wherein said individual unit
2 comprises one of a smart card, a personal area network (PAN) tool, and an
3 apparatus linked to a network.
- 1 48. The apparatus according to claim 44, wherein a subject's identity is
2 determined locally, under the subject's control, by having the subject provide
3 at least one of a user ID and by biometric identification of the subject among
4 enrolled authorized subjects being read by said reader, and
5 wherein said identification produces a set of N best matches for N
6 subsets, and an index formed by concatenation of the N indices uniquely
7 identifies the subject.

**METHOD AND APPARATUS FOR SECURE
AUTHORIZATION AND IDENTIFICATION USING
BIOMETRICS WITHOUT PRIVACY INVASION**

ABSTRACT OF THE DISCLOSURE

- 5 A method and apparatus for authenticating (or identifying)a subject, includes using one or a plurality of biometric measurements for authentication (or identification)without any sharing of the subject's biometric data with a party requesting authentication.

100

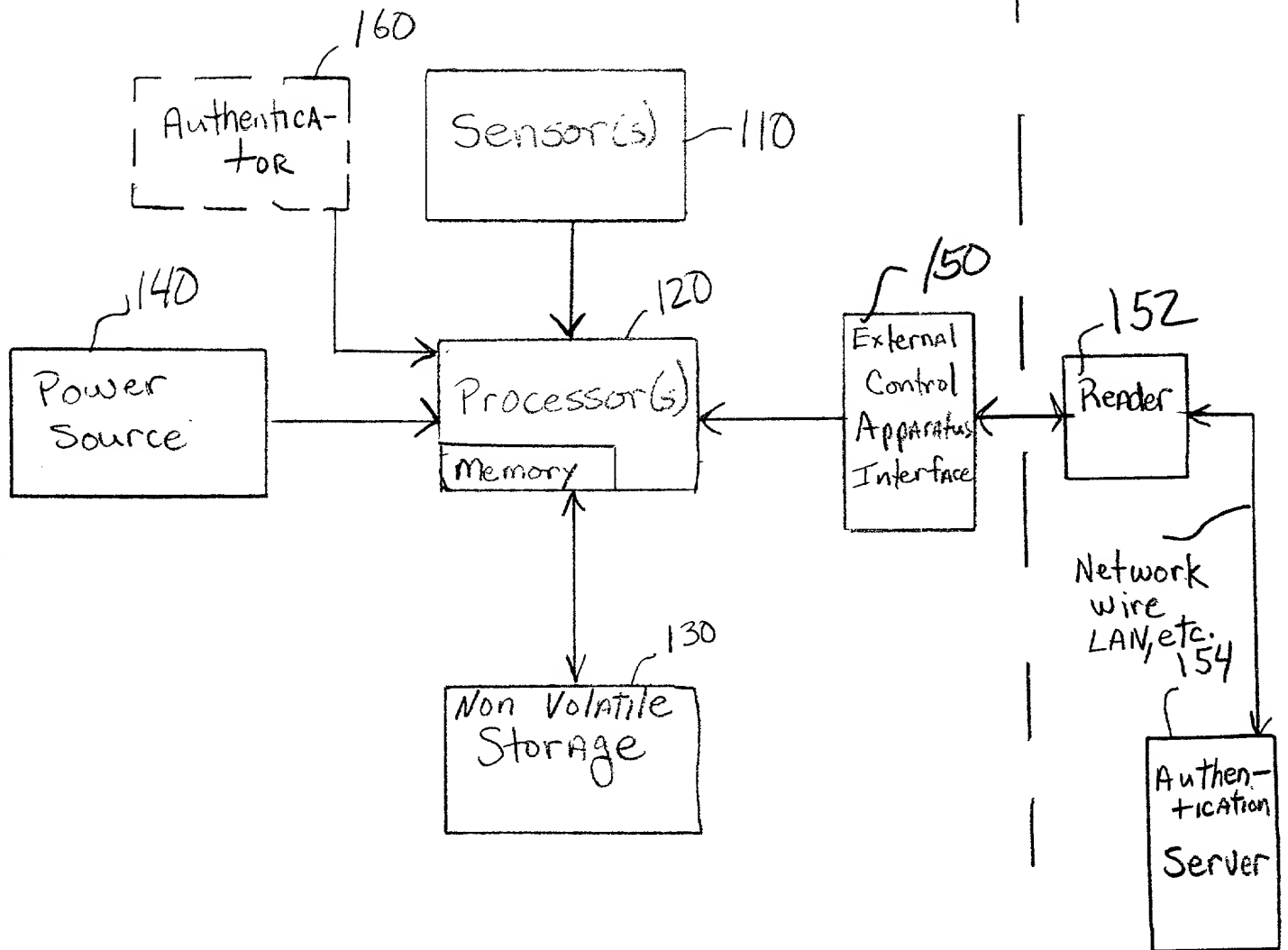


Fig. 1

Figure 2

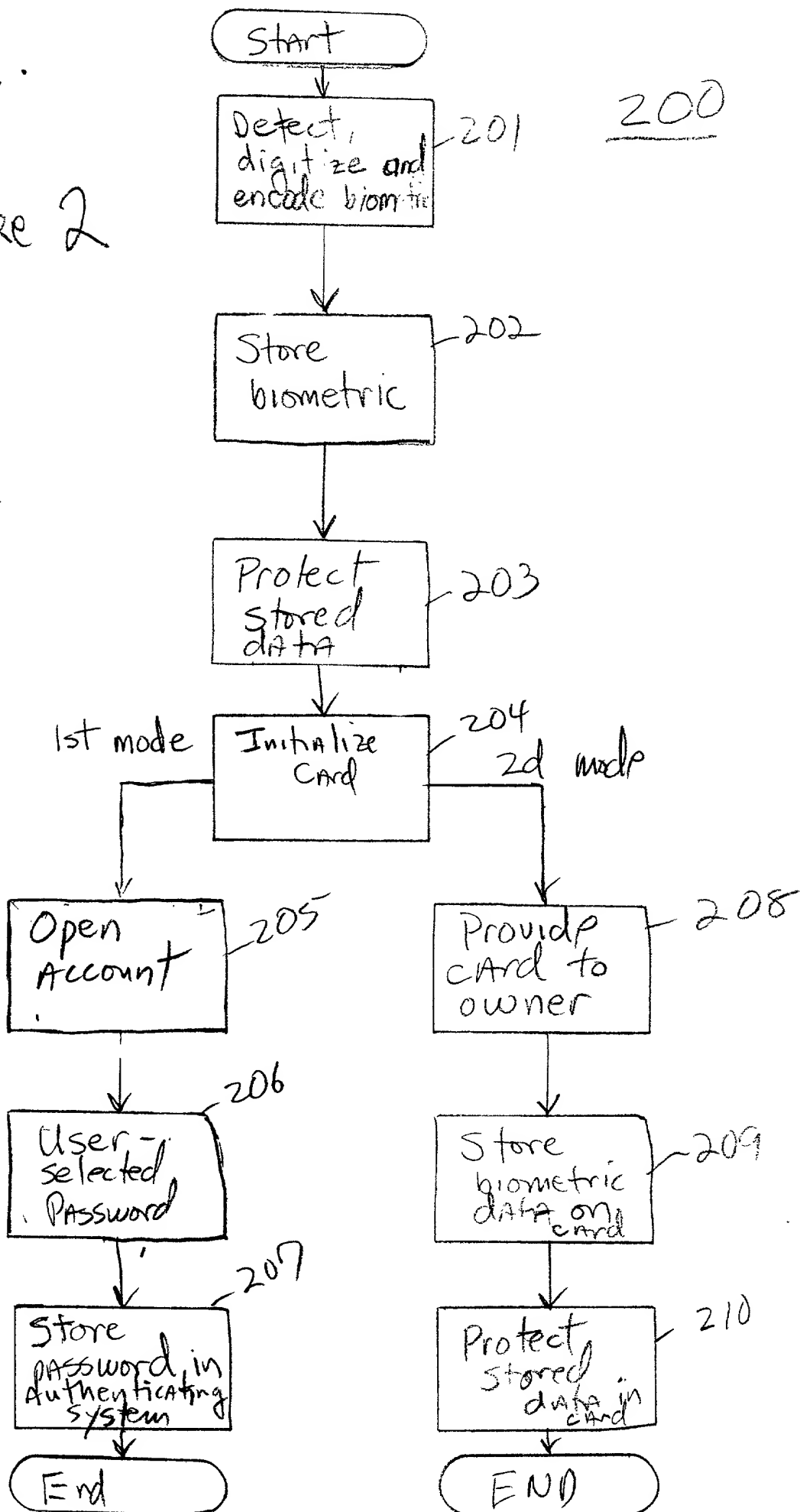
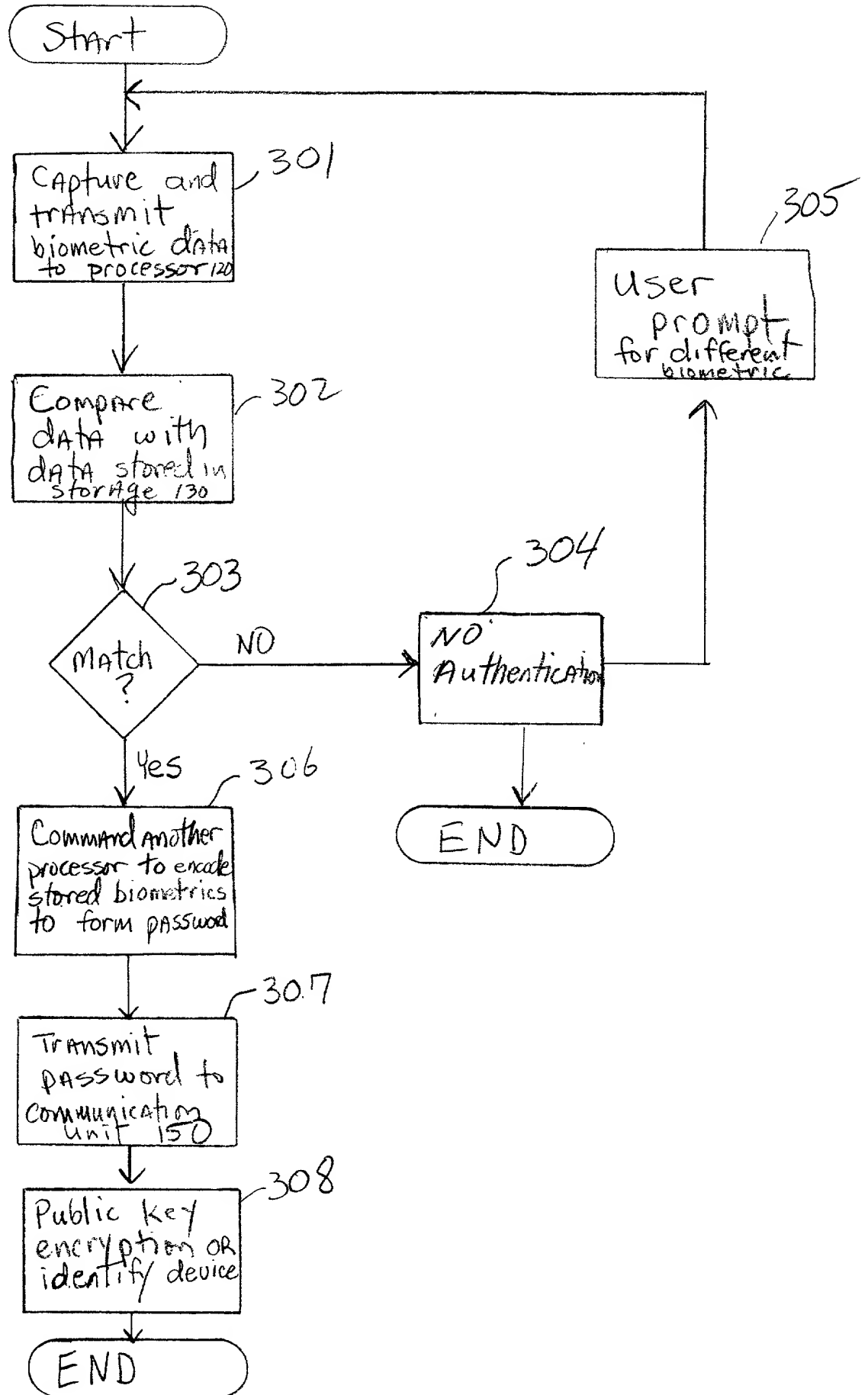


Figure 3

300



DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: METHOD AND APPARATUS FOR SECURE AUTHORIZATION AND IDENTIFICATION USING BIOMETRICS WITHOUT PRIVACY INVASION

the specification of which:
(check one)

☒ is attached hereto.

☐ was filed on _____, as Application Serial No. _____ and was amended on _____.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with Title 37, Code of Federal Regulations, § 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s):

Number	Country	Day/Month/Year	Priority Claimed
--------	---------	----------------	------------------

I hereby claim the benefit under Title 35, United States Code, § 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, § 112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, § 1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Prior U.S. Applications:

Serial No.	Filing Date	Status
------------	-------------	--------

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

As a named inventor, I hereby appoint the following attorneys and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: We hereby appoint Manny Schecter, Registration No. 31,722, Terry J. Ilardi, Registration No. 29,936, Christopher A. Hughes, Registration No. 26,914, Edward A. Pennington, Registration No. 32,588, John E. Hoel, Registration No. 26,279, Joseph C. Redmond, Jr., Registration No. 18,753, Douglas W. Cameron, Registration No. 31,596, Louis P. Herzberg, Registration No. 41,500, Kevin M. Jordan, Registration No. 40,277, Stephen C. Kaufman, Registration No. 29,551, Daniel P. Morris, Registration No. 32,053, Louis J. Percello, Registration No. 33,206, Jay P. Sbrolini, Registration No. 36,266, David M. Shoff, Registration No. 39,835, Paul J. Otterstedt, Registration No. 37,411 and Robert M. Trepp, Registration No. 25,933, to prosecute this application and transact all business in the United States Patent and Trademark Office connected therewith.

Send all correspondence to: **McGinn & Gibb, P.C., 1701 Clarendon Boulevard, Suite 100, Arlington, Virginia 22209. Customer No. 21254**

Telephone calls should be directed to Sean M. McGinn, McGinn & Gibb, P.C. at (703) 294-6699.

(1) Inventor: Timothy Joseph Chainer

Signature: _____ Date: _____

Residence: 161 Barrett Hill Road, Mahopac, New York 10541

Citizenship: United States of America

Post Office Address: Same as Above

(2) Inventor: Bruce P. Kitchens

Signature: _____ Date: _____

Residence: Millwood, New York 10546

Citizenship: United States of America

Post Office Address: P.O. Box 557, Millwood, New York 10546

(3) Inventor: Stephane Herman Maes

Signature: _____ Date: _____

Residence: 1 Wintergreen Hill Road, Danbury, Connecticut 06811

Citizenship: United States of America

Post Office Address: Same as Above

(4) Inventor: Marco Martens

Signature: _____ Date: _____

Residence: 104 S. Bedford Road, Chappaqua, New York 10514

Citizenship: Netherlands

Post Office Address: Same as Above

(5) Inventor: Joseph Dela Rutledge

Signature: _____ Date: _____

Residence: 11 Sycamore Terrace, Mahopac, New York 10541

Citizenship: United States of America

Post Office Address: Same as Above

(6) Inventor: Charles Philippe Tresser

Signature: _____ Date: _____

Residence: 953 West Boston Post Road, Mamaroneck, New York 10543

Citizenship: France

Post Office Address: Same as Above